REMARKS

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, 13-19, 22-27 and 29-38, and 41. Claims 2, 7-8, 12, 20-21, 28, 39 and 40 were canceled in a previous communication. By this paper, claims 13 and 41 are amended. No new matter is added. As such, claims 1, 3-6, 9-11, 13-19, 22-27, and 29-38, and 41 remain pending. In view of the following remarks, Applicants respectfully request reconsideration and allowance of all pending claims.

Claim Rejection Under 35 U.S.C. § 101

In the Office Action, the Examiner rejected claim 41 under 35 U.S.C. § 101 because the claimed invention is not limited to a single statutory subject matter class. Specifically, the Examiner stated:

> Although claim 41's preamble calls for a method of manufacturing a device, the limitations of the claim stray from such objectives, instead setting forth a memory containing bits, the writing of which allows for the enablement of a cryptographic subsystem.

Office Action, page 3. Applicants respectfully traverse this rejection.

Legal Precedent

The Supreme Court has recognized that the expansive language of Section 101 includes "anything under the sun that is made by man" as being statutorily patentable subject matter. *Diamond v. Chakrabarty*, 447 U.S. 303, 308-09 (1980). Several specific exceptions to statutorily patentable subject matter have been recognized and are limited to laws of nature, natural phenomena and abstract ideas. *See Diamond v. Diehr*, 450 U.S. 175, 185; 209 U.S.P.Q. 1, 7 (1981). Other than these specific exceptions, therefore, nearly anything man made is statutorily patentable subject matter under 35 U.S.C. §101.

As set forth above, and as noted by the Examiner, claim 41 is directed to a method of manufacturing a processor-based device, which is clearly statutory subject matter. Applicants assert further that the steps set forth in the method of claim 41 are within the statutory subject matter class of the method of manufacturing. Specifically, claim 41 recites a series of steps

associated with the method of manufacture, including: "providing a memory comprising a seed pool," "writing one or more bits of data to the seed pool," and "enabling a cryptographic security subsystem," among other things. Applicants respectfully assert that the recitation of such steps associated with a method of manufacturing a processor-based device clearly falls within the purview of patentable subject matter under Section 101 and, furthermore, that the steps are not in a separate statutory subject matter class, as asserted by the Examiner.

Applicants respectfully remind the Examiner that when examining claims for compliance with Section 101, the Examiner is to determine what Applicant has invented and is seeking to patent. *See* M.P.E.P. § 2106(II). As set forth in the specification of the instant application, a cryptographic subsystem may hinder the efficient assembly and testing of a device 100. *See* specification, page 23, lines 4-15. However, the security subsystem must be installed during manufacturing to ensure that the server 100 does not escape the secure manufacturing environment without proper safeguards. *Id.* at page 23, lines 17-22. To alleviate the concerns with the use of the security device 114 and to eliminate the inefficiencies introduced by the cryptographic security subsystem in the manufacturing environment, the security logic can be configured such that the security features are bypassed based on the state of the seed pool 122. *Id.* at page 24, lines 6-9. For instance, in one embodiment, the seed pool 122 initially may be populated during manufacturing with a pattern of bits having a known signature. *Id* at page 24, lines 9-10. During the manufacturing process the device 100 may be turned on and rebooted several times which may trigger the masking of one or more bits into the seed pool. *Id.* at page 24, lines 16-19. The security logic can be configured to remain in a bypass mode as long as the seed pool retains a predetermined amount of the signature value. *Id* at page 24, lines 20-23.

Accordingly, the specification discloses a method of manufacturing a processor-based device having the steps set forth in claim 41. Therefore, Applicants respectfully assert that claim 41 is limited to a single statutory subject matter class and, further, that explicit support for the steps recited for the method of claim 41 is disclosed in the specification. As such, Applicants respectfully request withdrawal of the rejection of claim 41 under Section 101.

Claim Rejection Under 35 U.S.C. § 112, second paragraph

In the Office Action, the Examiner rejected claim 41 as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. More specifically, the Examiner stated:

> Although the preamble of claim 41 calls for "a method of manufacturing a processor-based device," the Applicant fails to provide any steps or limitations regarding the manufacturing of a processor-based device, or any device for that matter.

Office Action, page 3. Applicants traverse the rejection.

Legal Precedent

The Examiner's focus during examination of claims for compliance with the requirement for definiteness of 35 U.S.C. 112, second paragraph, is whether the claim meets the threshold requirements of clarity and precision, not whether more suitable language or modes of expression are available. *See* M.P.E.P. § 2173.02. Although the Examiner may take exception to the terms used in the claims, the patentee may be his own lexicographer. *Ellipse Corp. v. Ford Motor Co.*, 171 U.S.P.Q. 513 (7th Cir. 1971), *aff'd.* 613 F.2d 775 (7th Cir. 1979), *cert. denied*, 446 U.S. 939 (1980). The Applicant may use functional language, alternative expressions, negative limitations, or any style of expression or format of claim which makes clear the boundaries of the subject matter for which protection is sought. *See* M.P.E.P. §§ 2173.01 and 2173.05; *In re Swinehart*, 439 F.2d 10, 160 U.S.P.Q. 226, (CCPA 1971). The Examiner is also reminded not to equate breadth of a claim with indefiniteness. *In re Miller*, 441 F.2d 689, 169 U.S.P.Q 597 (CCPA 1971).

The essential inquiry pertaining to the definiteness requirement is whether the claims set out and circumscribe a particular subject matter with a reasonable degree of clarity and particularity. *See* M.P.E.P. § 2173.02. As set forth in Section 2173 of the Manual of Patent Examining Procedure, definiteness of claim language must be analyzed, not in a vacuum, but in light of:

(A) The content of the particular application disclosure;
(B) The teachings of the prior art; and

(C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made.

In reviewing a claim for compliance with 35 U.S.C. 112, second paragraph, the examiner must consider the claim as a whole to determine whether the claim apprises one of ordinary skill in the art of its scope and, therefore, serves the notice function required by 35 U.S.C. 112, second paragraph, by providing clear warning to others as to what constitutes infringement of the patent. *See Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 1379, 55 U.S.P.Q.2d 1279, 1283 (Fed. Cir. 2000). Only when a claim remains insolubly ambiguous without a discernible meaning after all reasonable attempts at construction must a court declare it indefinite. *See Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings*, 370 F.3d 1354, 1366, 71 U.S.P.Q.2d 1081, 1089 (Fed. Cir. 2004). Accordingly, a claim term that is not used or defined in the specification is not indefinite if the meaning of the claim term is discernible. *See Bancorp Services, L.L.C. v. Hartford Life Ins. Co.*, 359 F.3d 1367, 1372, 69 U.S.P.Q.2d 1996, 1999-2000 (Fed. Cir. 2004).

Applicants fail to see how any of the three distinct steps set forth in the claim can be described as failing "to provide any steps or limitations regarding the manufacturing of a processor-based device, or any device for that matter," as stated by the Examiner. Office Action, page 3. Specifically, claim 41 sets forth a method of manufacturing a processor-based device which includes the steps of "providing a memory comprising a seed pool," "writing one or more bits of data to the seed pool," and "enabling a cryptographic security subsystem." As stated above, the specification provides detailed support for the steps recited in claim 41. Additionally, Applicants respectfully assert that one of ordinary skill in the art would understand the steps as set forth in the claim, as they are clear on their face and are supported by the specification. As such, Applicants respectfully assert that the claim is definite and sets forth steps for the method of manufacture of a processor-based device and respectfully request withdrawal of the rejection of claim 41 under Section 112, second paragraph, as being indefinite.

Claim Rejections Under 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, 13-19, 22-27, 29-38, and 41 under 35 U.S.C. § 102(e) as being anticipated by Saarinen, U.S. Publication No. 2002/0172359 (hereafter referred to as "the Saarinen reference"). Applicants respectfully traverse this rejections.

Legal Precedent

Anticipation under 35 U.S.C. § 102 can be found only if a single reference shows exactly what is claimed. *See Titanium Metals Corp. v. Banner*, 227 U.S.P.Q. 773 (Fed. Cir. 1985). For a prior art reference to anticipate under Section 102, every element of the claimed invention must be identically shown in a single reference. *See In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir.1990). That is, the prior art reference must show the *identical invention "in as complete detail as contained in the . . . claim"* to support a *prima facie* case of anticipation. *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989) (emphasis added). Thus, for anticipation, the cited reference must not only disclose all of the recited features but must also disclose the *part-to-part relationships* between these features. *See Lindermann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 486 (Fed. Cir. 1984). Accordingly, Applicants need only point to a single element or claimed relationship not found in the cited reference to demonstrate that the cited reference fails to anticipate the claimed subject matter. A *strict correspondence* between the claimed language and the cited reference must be established for a valid anticipation rejection.

Moreover, the Applicants submit that, during patent examination, the pending claims must be given an interpretation that is *reasonable* and *consistent* with the specification. *See In re Prater*, 162 U.S.P.Q. 541, 550-51 (C.C.P.A. 1969); *In re Morris*, 44 U.S.P.Q.2d 1023, 1027-28 (Fed. Cir. 1997); *see also* M.P.E.P. § 2111 (describing the standards for claim interpretation during prosecution). Indeed, the *specification* is "the primary basis for construing the claims." *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005). It is usually dispositive. *See id.* Interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *See In re Cortright*, 49 U.S.P.Q.2d 1464, 1468 (Fed. Cir. 1999); *see also* M.P.E.P. § 2111. That is, recitations of a claim must be read as they would be interpreted by those of ordinary skill in the art. *See Rexnord Corp. v.*

Laliram Corp., 60 U.S.P.Q.2d 1851, 1854 (Fed. Cir. 2001); *see also* M.P.E.P. § 2111.01. In summary, during prosecution an examiner must interpret a claim recitation as one of ordinary skill in the art would reasonably interpret the claim in view of the specification. *See In re American Academy of Science Tech Center,* 70 U.S.P.Q.2d 1827 (Fed. Cir. 2004).

The Saarinen Reference Lacks Features Recited in Independent Claims 1, 19 and 36

In rejecting claim 1, the Examiner stated, in pertinent part, "Regarding claim 1, Saarinen discloses a method of generating a cryptographic key for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) detecting occurrence of a first type of triggering event (par 32); (b) writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising a state bit indicative of a state of the seed pool (par 32) ... (e) examining the state bit to determine whether the seed pool is full (pars 33, 72)." Office Action, page 4. The Examiner indicated that claim 19 is rejected under similar rationale. *See id.* at page 6. Additionally, claim 36 is rejected under similar rationale. Applicants respectfully traverse the rejection.

Claim 1 recites, *inter alia,* "A method of generating a cryptographic key... the method comprising the acts of: (a) detecting occurrence of a first type of triggering event; (b) writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising *a state bit indicative of a state of the seed pool* ... (e) *examining the state bit to determine whether the seed pool is full.*" Claim 19 recites, *inter alia*, "A processor-based device comprising: security logic...wherein the security logic is configured to: detect the occurrence f a first type of triggering event; *examine the state bit to determine whether the seed pool is fully populated.*" Claim 36 recites, *inter alia*, "A method for restoring security data to a non-volatile memory in a computer system comprising...trackin the state of the seed pool to determine if the seed pool is fully populated, wherein tracking the state of the seed pool comprises *examining a state bit* that changes states when the seed pool is fully populated or *examining the position of a pointer* to determine wherein the portion of the non-volatile memory storing the seed pool is full." (Emphasis added).

In contrast to claims 1, 19 and 36, the Saarinen reference fails to disclose a state bit, much less examining a state bit to determine whether a seed pool is full. In the rejection of

the claims, the Examiner cited to paragraphs 33 and 72 of the Saarinen reference as disclosing such features. In their entirety, paragraphs 33 and 72 of the Saarinen reference state:

> [0033] Alternatively, the input entropy signals may be accumulated in an entropy accumulation pool as may be stored in persistent memory store 107. When a predetermined amount of entropy signals are stored in such pool, the accumulated signals may then be provided to the PRNG 104. Such process for providing accumulated signals is described further below in conjunction with FIG. 5B. The input entropy signals or accumulated entropy signals may be transmitted to the PRNG 104 at random or predetermined intervals in order to re-seed the PRNG 104 at random or predetermined intervals in order to re-seed the PRNG. Such re-seeding is discussed further below in conjunction with FIG. 5A.
> [...]
> [0072] FIG. 5B depicts an exemplary process 510 for determining when to transmit new input entropy to the PRNG 104 when entropy signals are accumulated. The process 510 begins at step 512 when the CPU 102 determines whether new input entropy is available. This may be done by searching an input entropy accumulation pool stored in persistent memory store 106. If there is no sufficient accumulation of input entropy (i.e. if a predetermined value of input entropy has not been stored), the process 510 continues to step516 where entropy is further accumulated in the entropy pool. If, on the other hand, sufficient input entropy has been stored, the process 510 continues to step 518 where the PRNG 104 is re-seeded, where newly determined state variables are based at least in part on the accumulated input entropy signals. The process 510 then ends.

As can be seen there is nothing in paragraphs 33 and 72 that can reasonably be considered to be a *state bit*, much less *examination of a state bit*. In particular, paragraph 33 simply discusses a "predetermined amount of entropy signals" being stored in a seed pool. *See* Saarinen at paragraph 33. Paragraph 72 discloses searching an input entropy accumulation pool to determine if new input entropy is available. *Id.* at paragraph 72. Thus, at best, the Saarinen reference discloses determining if a predetermined value of entropy has been stored. This does not indicate that a *state bit* is used or that a *state bit is examined* to determine if the seed pool is full. As such, for at least this reason, Applicants respectfully request withdrawal of the rejection under Section 102 and allowance of claims 1, 19 and 36, as well as all claims depending therefrom.

Additionally, with respect to claim 36, Applicants are unaware of, and the Examiner has not cited to, any portion of the Saarinen reference that can reasonably be considered the same as examining the position of a pointer to determine whether the portion of the non-volatile memory storing the seed pool is full. Accordingly, for at least this additional reason, Applicants respectfully request withdrawal of the rejection under Section 102 of claim 36 and allowance of the same, as well as all claims depending therefrom.

The Saarinen Reference Lacks Features Recited in Independent Claims 13, 27 and 41

As a preliminary matter, Applicants note that the rejection of claim 27 on page 7 of the Office Action actually cites to the Utz reference. However, there is no other reference to the Utz reference throughout the Office Action. Indeed, the Examiner indicated that all of the pending claims were rejected under Section 102 in view of the Saarinen reference. *See* Office Action, page 4. Additionally, the paragraph numbers cited in the rejection of claim 27 are the same paragraph numbers, for the most part, as those cited in rejecting claim 13 and which correlate to the paragraphs of the Saarinen, while the Utz reference is organized by columns and line numbers rather than by paragraph numbers. Accordingly, Applicants are assuming that the Examiner intended to cite to the Saarinen reference and not the Utz reference. The following arguments are based on this assumption. Therefore, if this assumption is incorrect, Applicants respectfully request that the Examiner issue another non-final Office Action clearly setting forth the basis of the rejection with citations to the specific column and line numbers of the Utz reference to which the Examiner is referring so that the Applicants may have a fair opportunity to respond to the rejection.

Claim 13 recites, *inter alia*, "A method of initializing a seed pool . . . comprising the acts of: (a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool, the plurality of bits having a signature value ... (c) writing one or more bits to the seed pool upon termination of the first type of triggering event, the one or more bits of data *altering the signature value of the seed pool*; [and] (d) enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered." (Emphasis added). Claim 27 recites, *inter alia*, "A processor-based device comprising . . . a non-volatile memory device to store a seed pool comprising a

plurality of data bits; and security logic in communication with ... the non-volatile memory device . . . wherein the security logic is configured to: write one or more bits to the seed pool, wherein the bits originate from a source external to the seed pool and *alter a signature value*; determine whether a plurality of data bits in the seed pool has at least a portion of the signature value; and disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value." (Emphasis added). Amended claim 41 recites, *inter alia*, "A method of manufacturing a processor-based device comprising ... writing one or more bits of data to the seed pool upon termination of a first type of triggering event, the one or more bits *altering the signature value*; and enabling a cryptographic security subsystem when more than a threshold amount of the signature value of the seed pool has been altered." (Emphasis added).

In contrast, the Saarinen reference does not teach or suggest the writing of one or more bits to a seed pool altering a signature value, as set forth in claims 13, 27 and 41. In rejecting claims 13, 27 and 41, the Examiner cited to paragraph 32 of the Saarinen reference as disclosing the above-mentioned feature. Paragraph 32 of the Saarinen reference, however, simply discloses capturing bits from random events and transmitting them as input entropy signals to a PRNG as an input seed. *See* Saarinen at paragraph 32. As such, Applicants are unaware of, and the Examiner has not cited to, anything in the Saarinen reference that can reasonably be considered a *signature value*, much less writing one or more bits to a seed pool to *alter a signature value*. Accordingly, for at least this reason, Applicants respectfully request withdrawal of the rejection of claims 13, 27 and 41.

Moreover, Applicants respectfully assert that the Saarinen reference fails to disclose *enabling the cryptographic security subsystem* when more than a threshold portion of the signature value of the seed pool has been altered, as set forth in claims 13 and 41. Additionally, the Saarinen reference does not disclose disabling "*establishment of the secure communication session* if the plurality of data bits has at least a portion of the signature value," as set forth in claim 27. As noted above, the Saarinen reference does not even disclose a signature value or anything that can reasonably be considered a signature value. Furthermore, Applicants are unaware of, and the Examiner has not cited to, any portion of Saarinen that can reasonably be considered *enabling a cryptographic security subsystem* or

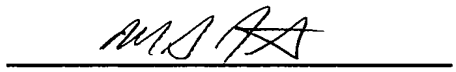
disabling establishment of a secure communication session based on the seed pool having a portion of the signature value. Accordingly, for these additional reasons, Applicants respectfully request withdrawal of the rejection under Section 102 of claims 13, 27 and 41, and allowance of the same, as well as all claims depending therefrom.

Conclusion

Applicants respectfully submit that all pending claims are in condition for allowance. However, if the Examiner wishes to resolve any other issues by way of a telephone conference, the Examiner is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: January 31, 2008



Michael G. Fletcher
Reg. No. 32,777
FLETCHER YODER
(281) 970-4545

Correspondence Address:
IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80527-2400